CLAIMS

1. A method for establishing and managing a trust model between an identification module and a radio terminal, characterized in that it comprises:

a terminal authentication step by said identification module, said identification step being carried out by means of identification means provided either to said identification module by a mobile radio-telephony network at the time of an initialization step or similar or at the time of a so-called updating step, or to said terminal by the identification module;

a control step by said module of at least one specific characteristic of the terminal, said specific characteristic being previously transmitted by radio-telephony to said module from a secured server of said mobile radio-telephony network.

2. The method according to Claim 1, wherein the lifetime of said terminal authentication means present in the identification module is limited by a determined expiration date, said authentication means being comprised of at least one authentication key.

3. The method according to Claim 1, wherein said identification module is an SIM type chip card or an USIM card for third – generation networks or an equivalent card comprising in a memory the representative subscription data.

4. The method according to Claim 1, wherein the identification module maintains a trust relationship with the radio terminal by generating authentication means and then by providing these authentication means to the radio terminal by secured exchange mechanisms based on authentication means initially available from the radio terminal.

5. The method according to Claim 1, comprising at the time of said initialization or updating step a generation step, carried out at least by

said identification module, of a so-called trust key, said trust key being used by said module for encrypting at least data exchanged between the identification module and the terminal.

6. The method according to Claim 2, wherein said initialization step of said authentication means is done on the initiative of the radio-telephony network, after denial of the key initiated by said module or the mobile radio-telephony network or the radio terminal, following an expiration of the validity period of the key or even at the time of initialization of the identification module.

7. The method according to Claim 1, wherein said authentication step comprises especially the following steps:

an utilization step in the terminal of at least one first authentication key memorized in the terminal by at least on first authentication algorithm memorized in the terminal, said first key having a validity period limited by a predefined expiration date;

an utilization step by the identification module of utilization of at least one second key memorized in the identification module by at least one second authentication algorithm memorized in the identification module, said second key being identical or complementary to the first key and associated with the terminal, said second key having a validity period limited by said predefined expiration date;

a comparison step in the identification module for comparing the results obtained by said first and second algorithms.

8. The method according to Claim 2, wherein the authentication step comprises the utilization of said predefined expiration date.

9. The method according to Claim 7, wherein said initialization step is initiated by a mobile radio-telephony network and also comprises:

generation by the identification module of at least one of said first and second keys;

a storage in the identification module of said second key;

transmission to the terminal by the identification module of said first key, said first key being encrypted by use of the trust key.

10. The method according to of Claim 7, wherein said comparison step is done between, on the one hand, a response produced by said first algorithm, stored in memory in the terminal and transmitted to said identification module and, on the other hand, a response result, stored in memory in the identification module, produced by said second algorithm.

11. The method according to Claim 7, wherein said first key is an asymmetrical private key Ks and said second key being a public key Kp complementary to the first key.

12. The method according to Claim 7, wherein said first key is symmetrical, said second key stored in memory in the identification module being identical to the first key, these keys forming a single symmetrical authentication key.

13. The method according to Claim 7, comprising an updating step of said first and second keys, initiated by the identification module prior to said predefined expiration, said updating step including the following sub-steps:

authentication between the terminal and the identification module using said first and second keys;

generation by an updating algorithm of the identification module of at least one updated key taking into account an information for replacing at least one of said first and second keys;

memorization in the identification module of the updated key for replacing said second key;

transmission to the terminal by the identification module of the updated key analogue of said first key.

14. The method according to Claim 13, wherein said updating step comprises in addition the control of at least one identifier of the terminal and / or of the identification module.

15. The method according to Claim 13, wherein an encryption of the key is carried out for said transmission to the terminal of the updated key analogue of the first key, said key encryption being done by said trust key.

16. The method according to Claim 13, wherein the updating step also comprises the following steps:

generation by the identification module of a new trust key after said authentication between terminal and module;

memorization in the identification module of the new trust key;

transmission to the terminal by the identification module of the newly generated trust key.

17. The method according to Claim 13, wherein said updating step is completed by a verification test comprising a return transmission on the part of the terminal of at least one datum representative of effective receipt of data transmitted by the identification module during the updating step.

18. The method according to Claim 5, wherein said trust key is a symmetrical encryption / decryption key analogous or identical to said symmetrical authentication key.

19. The method according to Claim 5, wherein said trust key is an erasable session key.

20. The method according to Claim 7, wherein a so-called revocation step is carried out on the initiative of the identification module, of the terminal, or of the corresponding radio-telephony network, said revocation step comprising the erasure in a memory of said identification module of at least said first key associated with the terminal.

21. An identification module in a terminal for the implementation of the method according to Claim 1, characterized in that it comprises means for memorizing at least one authentication key as well as at least one authentication algorithm, calculation means for executing at least one step consisting of applying said authentication key to said authentication algorithm memorized in the identification module, communication means, means for initiating a revocation and revocation means for revoking said authentication key, means for memorizing a specific characteristic of the terminal and means for actuating an updating algorithm for updating said authentication key, the communication means being capable of providing at least one authentication key to the terminal and receiving data send from a secured server of a mobile radio-telephony network.